



Microsoft 365 Playbook: Your Guide to Achieving True Cyber Resilience

Safeguard Microsoft 365 data against
an evolving threat landscape



Think Microsoft 365 Has You Covered? Think Again.

As enterprises increasingly adopt Microsoft 365 to power their collaboration and productivity, the volume of business-critical data stored in the cloud continues to surge. However, while Microsoft 365 offers robust infrastructure and service availability, significant gaps exist in its native data protection capabilities. Many organizations assume that data stored within Microsoft 365 is automatically safe from threats like ransomware, accidental deletions, and insider threats — this assumption is dangerously misleading. Gaining a clear understanding of Microsoft's Shared Responsibility Model is critical to safeguarding business-critical data from modern threats.

Microsoft's Shared Responsibility Model

Microsoft 365 operates under a Shared Responsibility Model, which clearly defines the roles and responsibilities between Microsoft and its customers. While Microsoft ensures the availability and uptime of its global cloud infrastructure, customers are responsible for protecting and securing their data.

"For all cloud deployment types, you own your data and identities. You're responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control."

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Shared	Shared	Customer	Customer
	Network controls	Shared	Shared	Customer	Customer
	Operating system	Shared	Shared	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

 Microsoft  Customer  Shared

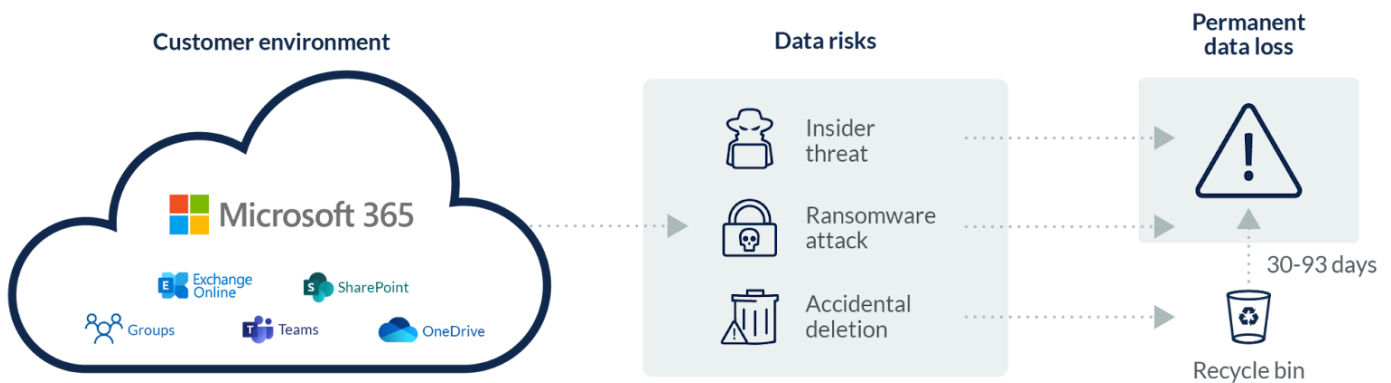
Many enterprises misunderstand this split, assuming Microsoft natively protects their data against all threats. In reality, Microsoft's built-in data protection mechanisms are designed primarily for service continuity, not for granular data recovery or long-term retention.

Understanding the Key Threats to Microsoft 365 Cyber Resiliency

Cyber threats targeting Microsoft 365 environments are intensifying. According to Microsoft's latest [Digital Defense Report](#), customers face a relentless barrage of over 600 million cyberattacks daily, with ransomware attacks surging by 195% since 2022.

Microsoft 365's built-in recovery mechanisms are not designed to withstand sophisticated ransomware attacks that can encrypt or permanently delete data. In fact, [70%](#) of ransomware incidents specifically target backups, and 43% of victims report their backups were encrypted, rendering native recovery tools ineffective. While retention policies may support short-term recovery, they are not a substitute for true backup or long-term data resilience.

Accidental or malicious deletions present another significant risk. Microsoft 365 offers limited recovery options, and once the retention window lapses, the data is permanently lost. This becomes especially dangerous in the face of insider threats—from departing employees to rogue administrators—who can delete, export, or manipulate sensitive information. Alarming, 21% of organizations still report data loss despite having Microsoft 365 backup policies in place, revealing how widespread and costly this misconception can be.



Limitations of Microsoft 365's Native Data Protection & Security

While Microsoft 365 includes features like geo-redundancy, versioning, recycle bin, and replication, these are designed to ensure service continuity—not to deliver comprehensive security, backup, or point-in-time recovery. The following critical gaps remain:

- **Short Retention Periods:** Microsoft 365 retains deleted data for only 14 to 93 days, with no flexibility to extend—leaving you unprotected once the window closes.
- **No Granular Recovery:** Native tools lack the ability to restore specific emails, files, or chats, forcing inefficient, broad rollbacks that disrupt users and delay recovery.
- **Ransomware Lockout & Malicious Deletions:** Without air-gapped or immutable backups, ransomware can encrypt or erase both live and backup data—making clean recovery nearly impossible.
- **Malicious Insider or Admin Threats:** A compromised or rogue admin can change retention settings or delete both primary and backup data, with no way to undo or trace the damage.
- **Operational Complexity:** Managing protection across Microsoft 365 workloads requires multiple admin consoles and scripts, making recovery slow, error-prone, and resource-intensive.

These limitations make a compelling case for enhanced, multi-layered data resilience strategies to safeguard Microsoft 365 environments from escalating threats.

Building Cyber Resilience for Microsoft 365

In today's rapidly evolving threat landscape, Microsoft 365 has become a high-value target for cybercriminals due to its widespread adoption and the vast amounts of business-critical, sensitive data it holds. Threat actors have grown increasingly sophisticated, using multi-vector strategies such as ransomware, social engineering, insider threats, and stealthy data exfiltration. Despite offering built-in availability and redundancy, Microsoft 365's native tools are not designed to defend against these complex attacks—leaving organizations exposed to data loss, operational downtime, and compliance violations.

A single layer of defense is no longer sufficient. To effectively secure Microsoft 365 environments, organizations must embrace a multi-layered cyber resilience strategy that spans immutable backups, infrastructure security, real-time threat detection, clean recovery, governance, and compliance. This approach goes beyond traditional backup, aiming to build an integrated defense framework that strengthens security posture across every layer of the data lifecycle.

Enterprises that fail to evolve their data protection strategy risk serious consequences—from regulatory penalties to prolonged business disruption. Multi-layered cyber resilience is no longer optional; it is foundational to operational continuity, data integrity, and digital trust. Achieving this level of readiness requires more than just technology—it calls for a clear, strategic roadmap that enables organizations to prevent threats, detect them early, and recover clean data with confidence.

Introducing Druva's Cyber Resilience Maturity Model for Microsoft 365

To help organizations confidently navigate today's escalating threat landscape, Druva has developed the Cyber Resilience Maturity Model for Microsoft 365—a structured, five-level framework that assesses your current posture and provides a clear roadmap toward advanced cyber readiness.

Whether you're just starting with basic backups or already implementing threat detection, the model enables you to benchmark maturity, identify gaps, and take targeted steps to strengthen Microsoft 365 data protection—progressing from immutability and secure infrastructure to proactive detection, cyber investigations, and automated recovery.

By aligning people, processes, and technology across these levels, organizations can build long-term, sustainable resilience. The model offers a practical foundation to measure progress, improve preparedness, and unify IT, security, and compliance efforts—making it an essential tool for any modern Microsoft 365 environment. Let's understand how these five levels work—and what they mean for your Microsoft 365 security posture.



Level 1: Data Immutability

This foundational stage focuses on ensuring that Microsoft 365 backup data cannot be altered or deleted, either intentionally or accidentally. By following the 3-2-1 backup strategy (three copies of data, on two different media, with one copy offsite), organizations build a resilient baseline that protects against ransomware, accidental deletions, and insider threats.

Impact:

- Guarantees data recoverability post-ransomware
- Eliminates the risk of permanent data loss due to accidental or malicious deletions
- Meets foundational backup best practices for Microsoft 365

How Druva Helps:

- **Air-Gapped Backups:** Stored outside your Microsoft 365 tenant for isolation.
- **Data Lock:** Prevents deletion, overwrites, or tampering of snapshots.
- **Zero Trust Architecture:** Built-in separation of duties and access boundaries.
- **3-2-1 Backup Support:** Enables multi-copy, multi-location protection strategies.

Level 2: Backup Security

Once data immutability is in place, the next priority is securing the backup infrastructure itself. Backups are only as safe as the environment they reside in. Protecting this layer prevents attackers from exploiting admin access or misconfigurations to delete or manipulate backups.

Impact:

- Protects backup configuration and metadata from compromise
- Prevents privilege escalation and internal abuse
- Streamlines secure access for IT and compliance teams

How Druva Helps:

- **RBAC (Role-Based Access Control):** Granular access across users, roles, apps, and workloads.
- **SSO & MFA:** Enforces strict authentication and identity verification.
- **Rollback Actions:** Instantly recover from internal sabotage or accidental deletions.

Level 3: Cyber Remediation

Securing data is just one part of the puzzle. Recovery must also be intelligent and clean. At this stage, organizations focus on separating clean data from impacted data and ensuring that restores don't reintroduce malware or ransomware.

Impact:

- Prevents malware reinfection during recovery
- Speeds up time to clean recovery with automated threat analysis
- Reduces dependency on external security tooling for recovery readiness

How Druva Helps:

- **Restore Scan:** Automatically scans recovery points for malware and IOCs.
- **Quarantine Bay:** Isolates infected snapshots to prevent the reintroduction of threats.
- **Curated Snapshots:** Creates "golden" restore points based on ransomware detection and data integrity.

Level 4: Cyber Investigation

After securing data and recovery paths, organizations must gain the ability to investigate incidents and understand how threats unfolded. This insight supports root cause analysis, regulatory response, and continuous improvement of cyber defenses.

Impact:

- Accelerates incident investigations and root cause analysis
- Strengthens security posture with actionable insights
- Supports audit readiness and regulatory response requirements

How Druva Helps:

- **Federated Search:** Swiftly locate IOCs and infected files across all Microsoft 365 workloads.
- **Audit Logs:** Trace user and admin activity to uncover unauthorized access.
- **Sensitive Data Governance:** Monitor, track, and defensibly delete exposed or regulated data.

Level 5: Enhance Detection

At the highest maturity level, organizations shift to proactive detection and real-time threat awareness. Rather than reacting to breaches, they detect threats early and respond quickly using automation and integrated security intelligence.

Impact:

- Enables early threat detection and faster response
- Reduces time to detect and contain breaches
- Complements SOC workflows with backup-layer intelligence

How Druva Helps:

- **Managed Data Detection & Response (DDR):** 24x7x365 cloud-based threat monitoring.
- **AI/ML-Based Anomaly Detection:** Flags suspicious activity across Microsoft 365 environments.
- **SIEM Integrations:** Built-in support for Microsoft Sentinel and Splunk for end-to-end visibility.

Most organizations today operate between Levels 1 and 2, relying on basic backup solutions without the visibility, automation, and investigative capabilities needed for full cyber resilience. But with ransomware, insider threats, and regulatory pressures on the rise, advancing through this maturity curve is no longer optional.

Druva's Cyber Resilience Maturity Model empowers enterprises to identify gaps, chart their progress, and build a security posture that's resilient by design.

Why Druva? The Enterprise Standard for Microsoft 365 Cyber Resilience



Trusted by over 4,000 enterprise customers, Druva delivers proven, large-scale data protection for Microsoft 365 environments. Organizations across industries rely on Druva to secure and manage massive volumes of cloud data while ensuring fast, clean recovery from ransomware, insider threats, and operational risks. At scale, Druva protects:

- 807,000+ SharePoint sites, the highest known for any single customer
- 31 TB in a single SharePoint site collection, supporting high-volume collaboration
- 55 million SharePoint items protected within a single site
- 258,000 Microsoft 365 groups, preserving structure and context across communication layers
- 172,000 Teams instances, ensuring conversations, files, and configurations are safeguarded
- Over 3 million mailboxes and 68 PB of Microsoft 365 data, making Druva one of the largest Microsoft 365 protection platforms globally

This scale demonstrates Druva's ability to handle complex, enterprise-class environments with ease, backed by cloud-native performance, zero infrastructure overhead, and built-in cyber resilience.

The Druva Advantage: Resilience Redefined for Microsoft 365

Long-Term Retention & Compliance

Druva delivers flexible, policy-based retention that extends far beyond Microsoft 365's native limits—enabling organizations to preserve data for years.

- Flexible, long-term retention with immutable backups
- Built-in compliance with zero-trust access controls
- Centralized policy enforcement

Fast, Granular Recovery

Druva delivers fast and granular recovery with curated snapshots that automatically identify the cleanest restore points for safe restoration.

- 99.9% data accuracy post-ransomware attacks
- Granular recovery for emails, files, chats, or full accounts in minutes
- Minimizes downtime and manual intervention during recovery

Built-in Ransomware & Threat Defense

Druva's 24x7x365 Managed Detection & Response (MDDR) strengthens your security posture with expert-led threat monitoring, accelerated containment, and proactive risk mitigation.

- 40% faster threat detection powered by AI and threat intelligence
- Real-time anomaly detection monitors over 3 million mailboxes and 68 PB of Microsoft 365 data
- 100% ransomware recovery assurance

Always-On, Out-of-Band Protection

Druva's cloud-native, air-gapped architecture ensures backup data remains isolated, immutable, and accessible—even during Microsoft 365 outages or credential compromise.

- Immutable, air-gapped backups prevent tampering
- Backup data remains accessible during Microsoft service disruptions
- Eliminates the need for physical infrastructure or manual isolation

As cyberattacks grow more sophisticated and recovery costs soar, legacy tools and fragmented protection are no longer enough. Organizations need a multi-layered approach to cyber resilience to safeguard Microsoft 365 data. Druva's Cyber Resilience Maturity Model delivers a clear, step-by-step path to modern protection — closing security gaps, minimizing downtime, and enabling true enterprise-scale resilience.

Next Steps

How are you identifying your organization's security gaps? [Take Druva's cyber resilience maturity assessment](#) today to get ahead of cyber threats.

See why Druva was recognized as a [2024 Gartner® Peer Insights™ Customers' Choice](#) for Enterprise Backup & Recovery Software Solutions and [start a risk-free 30-day free trial](#). No credit card required.

For more information

druva.com/solutions/microsoft-365-backup

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).